**First draft: Python for Penetesters learning Path**

**Refresher on Python:**

* Variables
* For Loops
* While Loops
* Input
* Conditionals
* Functions
* Ranges
* True-false,
* Input/Output,
* Lists, Control Flow
* Exception handling

**Common vulnerabilities Python can exploit**

* Buffer Overflow: Stack-based & heap-based
* Web App Authentication Bypass
* Code Injection
* Input Sanitation
* Weak Passwords

**Networks**

* Automate reconnaissance with Spider Foot: an OSINT tool written in Python
* How to Create a Python HTTP Banner Grabber
* Python Scripting for Port scanning
* Using the Socket Module for creating HTTP and HTTPS servers, clients, and revers shells
* Prepare for Wifi attacks by changing your MAC Address
* *Traffic sniffing & packet injection using a Kali Linux live-boot USB, an external Wifi adapter and Aircrack-ng\**
* *botnet filtering\**
* *Using machine learning to detect botnets\**
* Using Impacket for Privilege escalation on a Windows Domain Controller
* Exploring prebuilt tools in Python to bypass AV

**Attacking Web Applications:**

* Using SQL Map and Burp Suite to exploit Web forms and requests
* Cracking Password hashes with Hashcat
* How to build a web scrapper in Python plus using pre-built web scraping tools
* How to create a Email Sender
* Using the Social Engineering Toolkit for phishing